IS&T Questionnaire for Credit Unions With Less than $100 Million in Assets

Reference#	IS&T Audit Program Step	Example	Y/N / NA/ NR	Comments
Information Systems Strategy and Planning				
	Objective: To obtain reasonable assurance that information systems resources and strategies are sufficient to support the credit union's overall business objectives and strategies.			
	Summary Question: Has management committed the appropriate IS&T resources, and developed defined IS&T strategies, to facilitate achievement of the credit union's goals and objectives?			
EDPR_S1_005	Have long and short-term information systems strategies been formulated and approved by management to support the overall business strategy and technology requirements of the credit union?			
EDPR_S1_020	Does management monitor the adequacy of technical staff and related skills and experience?			
EDPR_S1_040	Is necessary training provided to all technical personnel?			
Relationship with Outsourced Vendors				
	Objective: To obtain reasonable assurance that management is appropriately managing outsourced vendor relationships in terms of service levels, pricing, and right of access.			
EDPR_S1_050	**Summary Question: Has management implemented an effective vendor management program?**			
EDPR_S1_050	Does management maintain a list of critical third party processors or outsourced vendors? If yes: Does this list indicate the service(s) provided and credit union personnel responsible for managing the relationship?	A list of critical vendors indicating the type of member information to which they have access. Examples include core system service providers, statement printers, VISA and debit card processors, ATM vendors, etc. Documentation describing how information is passed to and from the vendor (CD, leased communications line, secured Internet connection, etc.)		
EDPR_S1_065	Do selected vendors have to be approved by information technology and appropriate user management?			
Business Continuity Planning				

	Objective: To obtain reasonable assurance that appropriate backup, recovery, and contingency plans exist to ensure critical business processes will be restored in the event of a disaster.			
EDPR_S1_090	**Summary Question: Has management implemented an effective business continuity program?**			
EDPR_S1_090	Has management established and documented a Disaster Recovery Plan to ensure that essential information systems can be recovered in a timely manner?	A copy of the credit union disaster recovery plan including recovery of all critical systems, networks, communications, etc. Documentation of the analysis to determine what is critical vs. non-critical. Evidence of periodic updates.		
EDPR_S1_095	Is the Disaster Recovery Plan regularly tested and updated?			
EDPR_S1_100	Has management established and documented a Business Continuity Plan to ensure that essential non-systems related business processes can be recovered in a timely manner?			
EDPR_S1_105	Is the Business Continuity Plan regularly tested and updated?			
EDPR_S1_110	Do management and the users schedule the backup and retention of data as well as the erasure and release of media when retention is no longer required?	Evidence of backup and retention procedures, including off site transport of key backup media. Procedures and documentation to show destruction of expired tapes and other media.		
EDPR_S1_120	Is the readability of backup data periodically tested through restoration or other methods?			
EDPR_S1_125	Are backup media stored off-site and/or in a secure environmentally controlled location?			
EDPR_S1_130	Are backup media labeled to enable proper identification?			
Information Systems Operations				
	Objective: To obtain reasonable assurance that control activities related to computer operations provide for scheduled, monitored, and secured processing as well as timely identification of problems.			
EDPR_S2_005	**Summary Question: Has management implemented effective controls over its computer operations?**			
EDPR_S2_010	Is access to the job processing software appropriate and based upon user job responsibilities?			
EDPR_S2_020	Has management established a procedure to ensure that system problems are centrally recorded and monitored for timely resolution?			
EDPR_S2_025	If the credit union has agreement(s) with outside contractors and/or software vendors for technical support, does management monitor for compliance with these agreements?			

EDPR_S2_030	Does management provide for alternate sources of power (i.e., uninterruptible power supply, generators, etc.)?			
EDPR_S2_035	Has management implemented adequate smoke/fire detection and suppression devices?			
EDPR_S2_040	Are the environmental conditions of the data center (i.e., temperature, humidity) monitored and regulated?			
Operating System Support				
	Objective: To obtain reasonable assurance that operating system software within the technical environment is appropriately maintained.			
EDPR_S2_080	**Summary Question: Has management implemented an effective process to control operating system software activities?**			
EDPR_S2_080	Does management approve the acquisition and modification of operating system software to ensure compliance with system plans and strategies?			
EDPR_S2_085	Is the timing of changes to operating systems software coordinated with all affected parties to minimize the impact on other processing activities?			
EDPR_S2_090	Is current documentation for systems software available and used when installing and/or maintaining the software?			
EDPR_S2_095	Are all operating system acquisitions and modifications tested prior to implementation?			
EDPR_S2_100	Are vendor-issued operating system changes obtained from the vendor and implemented in a timely manner to ensure on-going support?			
EDPR_S2_105	Are back-out procedures for operating system changes developed and documented to allow the original environment to be restored if necessary?			
Application Development and Maintenance				
	Objective: To obtain reasonable assurance that changes to application systems are appropriately initiated, tested, approved, and migrated to the production environment.			
EDPR_S2_140	**Summary Question: Has management implemented an effective process to control application related activities?**			
EDPR_S2_140	Does management approve all decisions to purchase or develop application systems in order to ensure consistency with organizational plans and strategies?			
EDPR_S2_145	Does the credit union use a formal methodology or process to guide the acquisition, development, and maintenance of application systems?			
EDPR_S2_155	Is access to production environments appropriately restricted?			
EDPR_S2_165	Do system implementation procedures include training users on appropriate use of new or substantially modified systems?			
EDPR_S2_175	Is application source code as well as technical and user documentation maintained for executable production programs?			

EDPR_S2_180	Does management review and approve the conversion of data (e.g., balancing and reconciliation activities) from old application systems to new systems?			
EDPR_S2_185	Does management retain prior versions of application systems and/or data to allow for recovery of the environment in the event of processing problems?			
EDPR_S2_195	Does management ensure that supported versions of purchased application systems are being used and that new releases are implemented timely?			
Database Support				
	Objective: To obtain reasonable assurance that database software is appropriately maintained.			
EDPR_S2_205	Is responsibility for administration and definition of database components assigned to appropriate personnel?			
Information Systems Security				
	Objective: To determine whether the credit union has implemented a security strategy and related physical and logical access controls to ensure the adequate protection of credit union and member data at all times.			
EDPR_S3_005	**Summary Question: Has management implemented an effective security program to protect credit union and member information?**			
EDPR_S3_005	Has management established and documented an adequate information security policy to provide for the overall direction and implementation of information security?	A copy of the credit union Member Information Security Policy. Policy should address: Acceptable Use of Systems/Data. Access Request and Authorization, Workforce Clearance, Inventory of System/Data Assets, Board/Management/Individual Responsibilities, file and program security, patch management and system updates, firewall use and practices, remote access practices, logging and monitoring, incident response, periodic risk analysis and testing, physical security, special practices for portable computing equipment, media reuse and disposal, use of encryption, security training, anti-virus, vendor mgmt, vendor contract provisions, server and workstation		

		configuration standards, security program reporting, enforcement and sanctions.		
EDPR_S3_010	Are the roles and responsibilities related to information security administration appropriately defined and assigned?			
EDPR_S3_015	Has the ability to administer information security and make modifications to overall system security parameters been limited to appropriate personnel?			
EDPR_S3_020	Is the use of privileged security administrator accounts ("sysadmin" or "superuser") logged and reviewed?			
EDPR_S3_025	Have information security tools been activated to record and report security events (such as security violation reports) as defined in information security policies?	Evidence of security event logging on servers for items such as failed login attempts, account lock-outs, etc., also firewall traffic filter logging of unnecessary (blocked) network traffic. Evidence of adequate review and retention of these logs.		
EDPR_S3_030	Are these reports regularly reviewed and necessary corrective and disciplinary actions taken?			
EDPR_S3_035	Have vendor default passwords for operating system, application, communication, and network software been modified/changed?	Evidence that default passwords have been modified		
EDPR_S3_040	Are terminals and workstations used to process sensitive data protected by time-out facilities that are activated after a predetermined time period of inactivity?			

EDPR_S3_050	Are users (both local and remote) authenticated to the system through passwords or other authentication techniques?	Evidence of user authentication controls and control parameters such as passwords, smart tokens, biometric devices, etc.		
EDPR_S3_055	Does the use of passwords incorporate policies on periodic change, confidentiality, and password format (e.g. password length, alphanumeric content)?	Evidence of user authentication controls and control parameters such as password length, expiration, lockout threshold, etc.		
EDPR_S3_067	Are controls adequate to ensure the users' access privileges are consistent with their job responsibilities?			
EDPR_S3_070	Are access privileges immediately changed for employees who have changed responsibilities or been terminated?			
EDPR_S3_075	Is anti-virus software resident on all credit union’s computers and on any computer that is allowed to connect to the organization’s network?	Evidence that systems have anti-virus software installed, running, and using current versions of virus definition files as provided by the vendor		
EDPR_S3_080	Does virus software scan for viruses whenever downloading data or programs, opening data files, or executing programs?			
EDPR_S3_085	Are users required to periodically update virus signature files (lists) on their computers?			
EDPR_S3_090	Are controls in place which ensure that all software loaded on company computers is properly authorized and licensed?			
EDPR_S3_095	If unlicensed or unauthorized software is found, is appropriate action taken?			
EDPR_S3_100	Are appropriate physical restrictions in place for protected areas?	Evidence of appropriate controls which might include locks, keypad access, motion sensor or video camera monitoring		
EDPR_S3_105	Is the authority to modify physical access controls limited to appropriate personnel?			
Board Involvement				
	Objective: To determine whether the credit union has involved the Board of Directors in the Member Information Security process.			
Info Sec_S1_1	1. Has the board or its designated committee approved a written Corporate Information Security Program that meets the objectives of the Information Security Guidelines (guidelines)?			

Info Sec_S1_2	2. If the board has assigned responsibility for program implementation and review of management reports to an individual or committee, do they possess the necessary knowledge, expertise and authority to perform the task?			
Info Sec_S1_4	3. If more than one information security program exists for the institution, are the programs coordinated across organizational units?			
Info Sec_S1_5	4. Determine the usefulness of reports from management to the board (or its designated committee). Does the report adequately describe the overall status of the program, material risk issues, risk assessment, risk management and control decisions?	Evidence of reporting to the board as found in board meeting minutes including, but not limited to significant changes in the information security infrastructure or environment, annual review of the risk assessment, test of key controls, etc.		
Info Sec_S1_6	5. How often does the board (or its designated committee) review reports?			
Risk Assessment				
	Objective: To determine whether the credit union has assessed risk to the confidentiality, integrity, and availability of member information and information systems.			
Info Sec_S2_1	1. Does the institution assess risk to its member information systems and non public member information?			
Info Sec_S2_6	2. Does the institution identify all reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of member information or member information systems?	A copy of the credit union risk assessment document, listing reasonable internal and external threats, controls to mitigate the threats, a rating of the probability and impact of the threat (given the controls), and a conclusion regarding the risk as acceptable or unacceptable with an action plan.		
Info Sec_S2_7	3. Does the institution support its estimate of the potential damage posed by various threats?			
Info Sec_S2_8	4. Review the institution’s existing controls to mitigate risks. Does the institution’s analysis consider the current administrative, physical, and technical safeguards that prevent or mitigate potential damage?			
Info Sec_S2_9	5. Does the institution use test results to support its assessment of the adequacy and effectiveness of those controls?			

Info Sec_S2_10	6. Does the institution identify and prioritize its risk exposure, decide on the risks it must mitigate, and create a mitigation strategy?	Evidence of risk mitigation strategy, such as review of results of risk assessment or testing of key controls and making corrections or adjustments. Detailed tracking to resolution for any significant or moderate findings.		
Info Sec_S2_11	7. Is the decision to accept risks documented and reported to the appropriate management levels?			
Info Sec_S2_15	8. Does the risk assessment include vendor oversight requirements?			
Adequacy of the Program to Manage and Control Risk				
	Objective: To determine the adequacy of the Member Information Security Program to manage and control risk.			
Info Sec_S3_1	1. Review internal controls and policies. Has the institution documented or otherwise demonstrated, at a minimum, that it considered the following controls, and adopted those it considered appropriate:			
	(a) Encryption of electronically transmitted and stored member data?	Evidence of encryption such as PGP or some other secure algorithm for all member information transmitted via the Internet. Evidence of analysis to determine what should and should not be encrypted.		
	(b) Procedures to ensure that systems modifications are consistent with the approved security program?	Evidence of procedures for system modification, generally including approval, testing, implementation and documentation of all changes		
	(c) Dual control procedures, segregation of duties, and employee background checks?	Evidence of sufficient dual control for core systems processes such as file maintenance and override reports, background checks for all new hires		
	(d) Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into member information systems?	Evidence of monitoring either Intrusion Detection Systems or manually monitoring server logs and firewall logs for attempted intrusions		
	(e) Measures to protect against destruction, loss, or damage of information from potential environmental hazards, such as fire and water damage or technological failures?	Evidence of appropriate fire detection and suppression equipment, climate control, power conditioning equipment, etc., for areas containing critical systems		

Info Sec_S3_3	2. Are key controls, systems, and procedures of the information security program regularly tested by independent third parties or qualified independent staff in accordance with the risk assessment?	Most recent report from any third party testing of key controls and management responses if applicable		
Info Sec_S3_7	3. Does management take appropriate steps to address adverse test results?			
Service Provider Oversight				
	Objective: To determine the effectiveness of credit union measures to oversee service providers.			
Info Sec_S4_3	1. Do contracts require service providers to implement appropriate measures to meet the objectives of the guidelines?	A copy of current contracts for vendors having access to member information which includes obligatory language regarding the protection of such information. Documentation of analysis indicating that all contracts have been reviewed for compliance.		
Info Sec_S4_4	2. Does the credit union's risk assessment require monitoring a service provider?			
Info Sec_S4_5	3. Do service provider contracts provide for sufficient reporting from the service provider to allow the credit union to appropriately evaluate the service provider’s performance and security, both in ongoing operations and when malicious activity is suspected?			
Info Sec_S4_7	4. Does the credit union review the financial condition of service providers?			
NOTE: Exam Core refers to the items that are the core of the IS&T examination audit program. All credit unions regardless of complexity and size should focus on the 16 items identified as exam core questions (salmon colored questions). In addition, several questions are identified as significant only to larger credit unions, such as those with $100 million in assets or more. The IS&T exam will certainly cover the 16 core exam items, however, credit union personnel should be prepared to speak to all topics absent of any designation in this column as time permits.				